

VoIP forensics: un caso pratico di intercettazione

Ing. Vandone Roberto



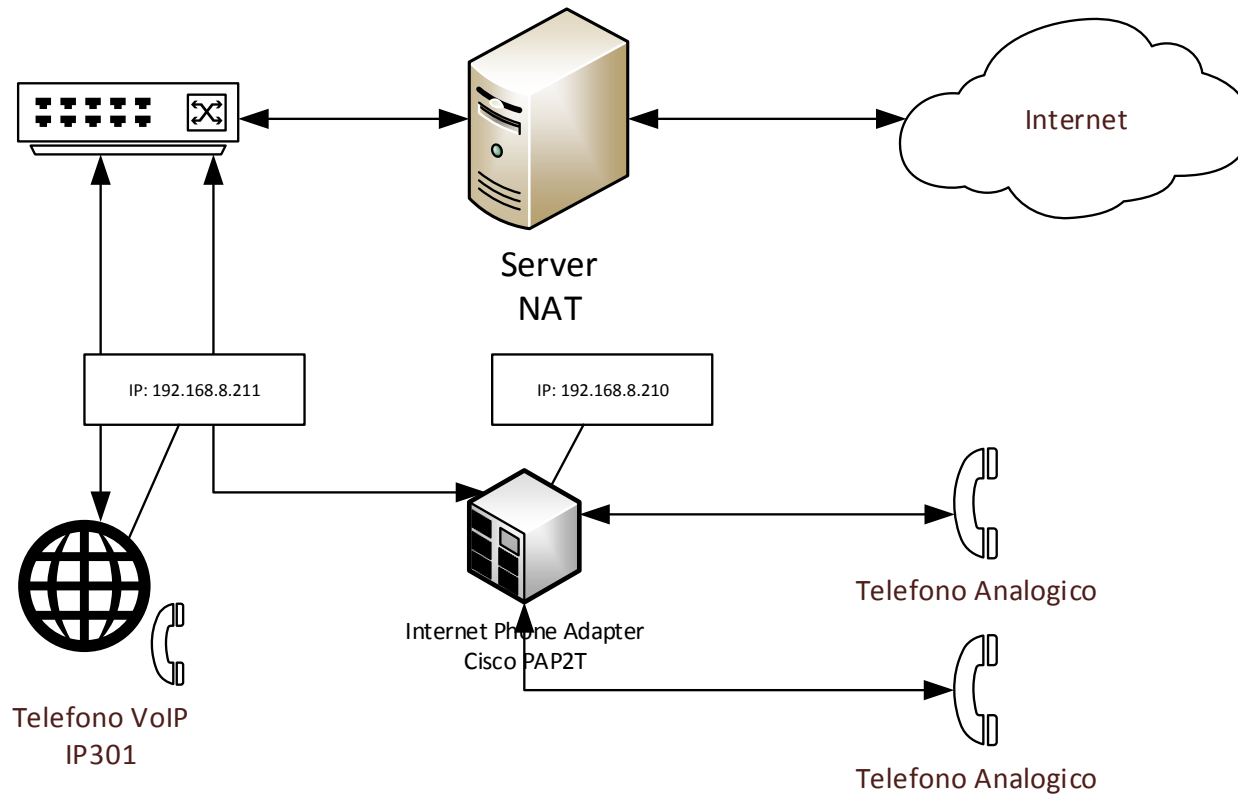
VoIP

- ▶ Il VoIP, Voice over IP, identifica una tecnologia che permette di effettuare una conversazione telefonica sfruttando una connessione Internet o, più in generale, una qualsiasi rete dati che utilizzi il protocollo IP.
- ▶ Grazie inoltre a numerosi provider VoIP, è possibile effettuare chiamate anche da e verso la rete telefonica tradizionale.

Vantaggi VoIP

- ▶ costi inferiori per le chiamate, specialmente sulle lunghe distanze;
- ▶ costi contenuti dell'infrastruttura, basta una rete IP;
- ▶ possibilità di avere maggiori funzionalità, ad esempio numeri diversi su un unico collegamento;
- ▶ salvataggio dei messaggi su PC;
- ▶ telefonate gratuite tra utenti dello stesso fornitore o fornitori convenzionati;
- ▶ possibilità di implementare un centralino interno utilizzando solo del software;
- ▶ possibilità di fare conferenze.
- ▶

Topologia rete



Telefono VoIP IP-301

L'IP 301 è un telefono VoIP molto semplice e diffuso, ha un connettore RJ-45 per permettere il collegamento a Internet e un secondo connettore RJ-45 per permette l'eventuale collegamento diretto ad un PC, infine è presente il connettore per l'alimentazione.



Phone Adapter Cisco PAP2T

Il PAP2T è un dispositivo economico e molto piccolo, circa 10x10x2,8 cm, ha una porta RJ-45 per il collegamento alla rete, 2 porte RJ-11 per il collegamento ai telefoni analogici e una porta per l'alimentazione. Sono inoltre presenti 4 led che indicano lo stato di funzionamento del dispositivo.



Intercettazione traffico VoIP

No.	Time	Source	Destination	Protocol	Length	Info
21	62.9299200	83.211.227.21	192.168.8.210	SIP/SDP	1379	Request: INVITE sip:[REDACTED]@192.168.[REDACTED].61139

Session Initiation Protocol (INVITE)

- Request-Line: INVITE sip:[REDACTED]@192.168.[REDACTED]:61139 SIP/2.0
- Message Header
 - Record-Route: <sip:83.211.227.21;lr;ftag=8DB8C91C-1FA8;did=f751.84dc6947>
 - Via: SIP/2.0/UDP 83.211.227.21:5060;branch=z9hg4bk1549.a487841.0
 - Via: SIP/2.0/UDP 83.211.2.220:5060;rport=63740;received=83.211.2.220;x-route-tag="tgrp:slot6";branch=z9hg4bkD6F1AB2380
 - From: <sip:[REDACTED]@83.211.2.220>;tag=8DB8C91C-1FA8
 - SIP from address: sip:347[REDACTED]@83.211.2.220
 - SIP from address User Part: 347[REDACTED]
 - SIP from address Host Part: 83.211.2.220
 - SIP from tag: 8DB8C91C-1FA8
 - To: <sip:[REDACTED]@voip.eutelia.it>
 - SIP to address: sip:[REDACTED]@voip.eutelia.it
 - Call-ID: 9CD27DFB-15F811E5-89C1B8CD-9198FD9D@83.211.2.220
 - User-Agent: Cisco-SIPGateway/IOS-12.x
 - Allow: INVITE, OPTIONS, BYE, CANCEL, ACK, PRACK, COMET, REFER, SUBSCRIBE, NOTIFY, INFO, UPDATE, REGISTER
 - CSeq: 101 INVITE
 - Max-Forwards: 9
 - Remote-Party-ID: <sip:[REDACTED]@83.211.2.220>;party=calling;screen=yes;privacy=off
 - Contact: <sip:[REDACTED]@83.211.2.220:63740>
 - Contact URI: sip:[REDACTED]@83.211.2.220:63740
 - Expires: 180
 - Allow-Events: telephone-event
 - Content-Type: application/sdp
 - Content-Length: 441

Chiamata da numero esterno

Intercettazione traffico VoIP

No.	Time	Source	Destination	Protocol	Length	Info
71	109.805110	83.211.227.21	192.168.8.210	SIP	404	Status: 200 OK
72	170.029723	83.211.227.21	192.168.8.210	SIP/SDP	1266	Request: INVITE sip:[REDACTED]@192.168.[REDACTED]:61139

<

Session Initiation Protocol (INVITE)

- Request-Line: INVITE sip:[REDACTED]@192.168.[REDACTED]:61139 SIP/2.0
- Message Header
 - Record-Route: <sip:83.211.227.21;lr;ftag=25820DD4-1F9C;did=c4a.46d1a5e>
 - Via: SIP/2.0/UDP 83.211.227.21:5060;branch=z9hg4bkd198.24f64474.0
 - Via: SIP/2.0/UDP 62.94.71.96:5060;rport=52307;received=62.94.71.96;x-route-tag="tgrp:slot6";branch=z9hg4bk5F0C0C167F
 - From: <sip:62.94.71.96>;tag=25820DD4-1F9C
 - SIP from address: sip:62.94.71.96
 - SIP from address Host Part: 62.94.71.96
 - SIP from tag: 25820DD4-1F9C
 - To: <sip:[REDACTED]@voip.eutelia.it>
 - Call-ID: DCA884E1-15F811E5-9CD888A0-4C092B3@62.94.71.96
 - User-Agent: Cisco-SIPGateway/IOS-12.x
 - Allow: INVITE, OPTIONS, BYE, CANCEL, ACK, PRACK, COMET, REFER, SUBSCRIBE, NOTIFY, INFO, UPDATE, REGISTER
 - CSeq: 101 INVITE
 - Max-Forwards: 9
 - Contact: <sip:62.94.71.96:52307>
 - Expires: 180
 - Allow-Events: telephone-event
 - Content-Type: application/sdp
 - Content-Length: 442
 - P-hint: 2 Niente 2
- Message Body

Chiamata da numero nascosto

Intercettazione traffico VoIP

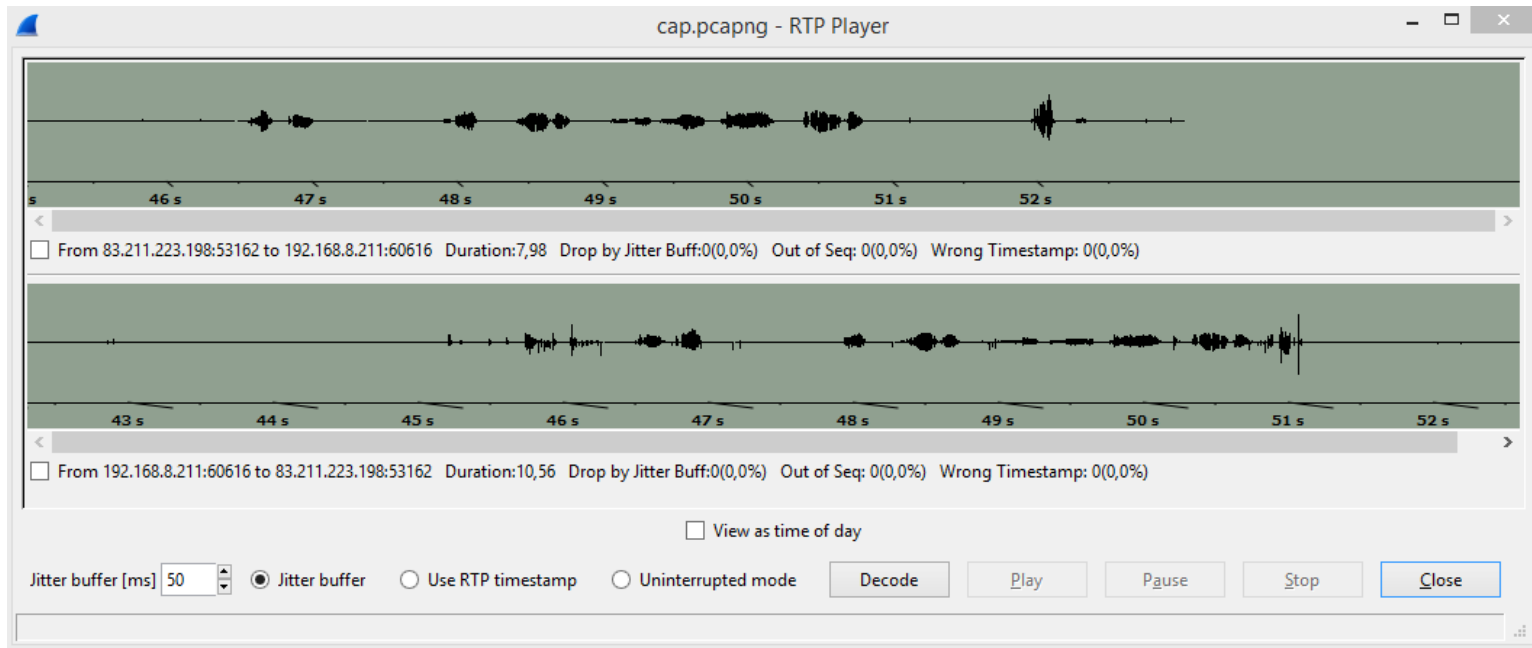
No.	Time	Source	Destination	Protocol	Length	Info
12	37.902520	83.211.227.21	192.168.8.211	SIP/SDP	1249	Request: INVITE sip:0[REDACTED]@192.168.8.211:61760
Session Initiation Protocol (INVITE)						
Request-Line: INVITE sip:0[REDACTED]@192.168.8.211:61760 SIP/2.0						
Message Header						
Record-Route: <sip:83.211.227.21;lr;ftag=23116df4f445b5fdo1;did=a5b1.20c46952>						
Via: SIP/2.0/UDP 83.211.227.21:5060;branch=z9hg4bka2a7.14858976.0						
Via: SIP/2.0/UDP 192.168.8.210:5061;received=195.72.216.66;branch=z9hg4bK-54f2c8f5;rport=63157						
From: Anonymous <sip:anonymous@voip.eutelia.it>;tag=23116df4f445b5fdo1						
To: <sip:0[REDACTED]@voip.eutelia.it> Call-ID: c76d7a80-489032e1@192.168.8.210						
CSeq: 102 INVITE Max-Forwards: 16						
Contact: 0[REDACTED] <sip:0[REDACTED]@195.72.216.66:63157> Expires: 240 User-Agent: Linksys/PAP2-3.1.3(LS) Content-Length: 430 Allow: ACK, BYE, CANCEL, INFO, INVITE, NOTIFY, OPTIONS, PRACK, REFER Supported: 100rel, x-sipura Content-Type: application/sdp						
P-hint: Geo Onnet from Prepaid						
Message Body						

Chiamata da numero nascosto di Eutelia

Intercettazione della password

```
test@kali: ~  
File Modifica Visualizza Cerca Terminale Aiuto  
* Dumped login from 83.211.227.21 -> 192.168.8.211 (User: '03211856066')  
* Dumped login from 83.211.227.21 -> 192.168.8.211 (User: '03211856066')  
* Dumped login from 83.211.227.21 -> 192.168.8.211 (User: '03211856066')  
  
* Exiting, sniffed 3 logins  
test@kali:~$ sipcrack -w psw auth.txt  
  
SIPcrack 0.2 ( MaJoMu | www.codito.de )  
-----  
  
* Found Accounts:  
  
Num      Server          Client          User      Hash|Password  
-----  
1        192.168.8.211  83.211.227.21  03211856066  43... d  
2        192.168.8.211  83.211.227.21  03211856066  97! ... J3796f4)  
3        192.168.8.211  83.211.227.21  03211856066  9759... 96f4 3  
  
* Select which entry to crack (1 - 3): 2  
  
* Generating static MD5 hash... b...7b61124...J3490...00,33323  
* Loaded wordlist: 'psw'  
* Starting bruteforce against user '03211856066' (MD5: '9;...J3d...474 33  
7...20')  
* Tried 13 passwords in 0 seconds  
  
* Found password: '...'  
* Updating dump file 'auth.txt'... done  
test@kali:~$
```

Intercettazione audio



Conclusioni

- i protocolli SIP e RTP sono molto semplici da analizzare perché in chiaro e si prestano a fornire molteplici elementi utili alle investigazioni.
- è possibile sfruttare le credenziali altrui per «duplicare» un'utenza VoIP.
- trattandosi di dispositivi di rete soffrono inoltre dei problemi classici dei normali device di rete.

Contatti: roberto.vandone@gmail.com